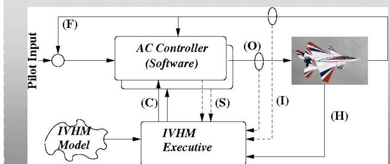
National Aeronautics and Space Administration

INTEGRATED SOFTWARE HEALTH MANAGEMENT FOR AIRCRAFT GN&C

Johann Schumann[1], Ole Mengshoel[2]



Principle architecture for ISWHM

Abstract

Modern aircraft rely heavily on dependable operation of many safety-critical software components. Despite careful design, verification and validation (V&V), on-board software can fail with disastrous consequences if it encounters problematic software/hardware interaction or must operate in an unexpected environment.

We are using a Bayesian approach to monitor the software and its behavior during operation and provide up-to-date information about the health of the software and its components. The powerful reasoning mechanism provided by our model-based Bayesian approach makes reliable diagnosis of the root causes possible and minimizes the number of false alarms. Compilation of the Bayesian model into compact arithmetic circuits makes SWHM feasible even on platforms with limited CPU power. We show initial results of SWHM on a small simulator of an embedded aircraft software system, where software and sensor faults can be injected.

References

[1] J. Schumann, O. Mengshoel, and T. Mbaya. Integrated Software and Sensor Health Management for Small Spacecraft. Proc. of SMC-IT, IEEE, 2011

[2] A. Srivastava and J. Schumann. The Case for Software Health Management Proc. of SMC-IT, IEEE, 2011

[3] J. Schumann, O. Mengshoel, A. Srivastava and A. Darwiche. Towards Software Health Management with Bayesian Networks. In Proc. FSE (Future of Software Engineering), ACM, 2010.

[4] K. Pipatsrisawat, A. Darwiche, O. Mengshoel, and J. Schumann. Software Health Management: A Short Review of Challenges and Existing Techniques. In Workshop Software Health Management, SMC-IT, 2009.

Software Can Fail

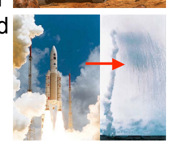
Despite careful SW development and V&V, safety-critical SW can fail.

F-22 Raptors crossing the date-line: SW bug caused loss of navigation and communication

Harrier Autolander: buggy radar-altimeter integration caused near-crash during landing (NASA)

SPIRIT: overfull on-board file system caused reboot-loop after landing

Ariane-V: SW reused from Ariane IV caused overflow and destruction of rocket



Software Health Management *monitors* the system and software during operation to

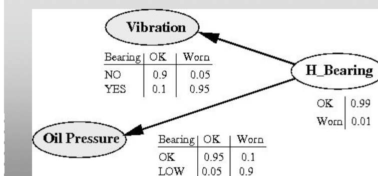
- realiably *detect* faults
- *diagnose* most likely root cause(s) while minimizing the number of false alarms and missed adverse events

A Bayesian ISWHM

We are using Bayesian networks (BN) to construct a model of the software and its behavior in nominal and failure cases. BNs can be used to

- detect failure(s), and to
- perform detailed reasoning on the root cause of the problem

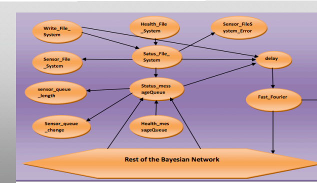
Example: low oil pressure *and* vibration indicates a likely problem with a bearing.



Simple Bayesian network

Modeling for ISWHM

ISWHM models are constructed from (software) sensor nodes, unobservable status nodes, and health nodes. Low posteriors of health nodes indicate problems and poor SW health.

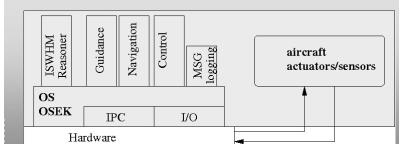


Bayesian ISWHM submodel

ISWHM Demonstration System

For demonstration, we developed a small embedded system/SW simulator, where faults can be easy injected

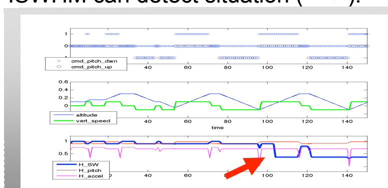
- Plant model: open NASA F-16 model
- Operating System: OSEK (simple real-time OS widely used in automotive industry) simulator to show suitability for small systems (UAV)
- simple GN&C with failure injection
- IVHM task uses arithmetic circuits



OSEK tasks for ISWHM demonstrator

Results for Example Scenario

Writes to almost full on-board file system can cause delays in the control loop (if "badly" implemented), which can result in aircraft oscillations similar to dangerous PIO (pilot induced osc.). ISWHM can detect situation (→).



ISWHM: SW health drops indicating problem in SW

[1] SGT, INC, NASA Ames [2] CMU, NASA Ames with contributions by Timmy Mbaya, Umass, Boston/USRP

NASA Aviation Safety Annual Technical Meeting, St. Louis, MO May 10 – 12, 2011